(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 631 038 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
01.03.2006 Bulletin 2006/09

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(21) Application number: **05018691.5**

(22) Date of filing: **29.08.2005**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **28.08.2004 KR 2004068280**

(71) Applicant: **LG Electronics Inc.**
Yongdungpo-gu
Seoul (KR)

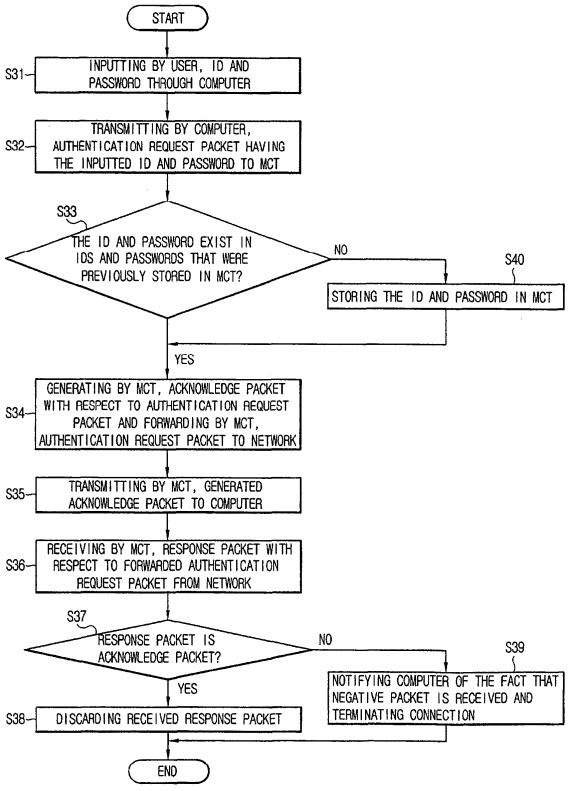
(72) Inventor: **Cho, Young-Beack**
Yongdungpo-Gu
Seoul (KR)

(74) Representative: **von Hellfeld, Axel**
Wuesthoff & Wuesthoff
Patent- und Rechtsanwälte
Schweigerstrasse 2
81541 München (DE)

(54) Authentication system and method thereof for a dial-up networking connection via terminal

(57) Disclosed are an authentication system and method thereof for a dial-up networking connection via a terminal. The authentication system includes a terminal for snooping an authentication request packet that includes an authentication ID and password of a computer requesting authentication, and for generating an acknowledge packet of the authentication request packet. The authentication method includes receiving an authentication request packet including an authentication ID and password by a terminal, generating an acknowledge packet by the terminal, and transmitting generated acknowledge packet from the terminal to the computer.

FIG. 3



EP 1 631 038 A2

Description

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of earlier filing date and right of priority to Korean Application No. 10-2004-68280, filed on August 28, 2004, the contents of which are hereby incorporated by reference herein in its entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to a dial-up networking connection via a terminal, and particularly, to an authentication system and method thereof for a dial-up networking connection via a terminal.

BACKGROUND OF THE INVENTION

[0003] Figure 1 illustrates an authentication processing procedure for a dial-up networking connection via a terminal in accordance with the conventional art.

[0004] Conventionally, to use a dial-up networking connection service, an authentication module in computer 1 transmits an authentication request packet (PAP_Authenticate_Request) to a mobile communications terminal 2, which then retransmits the authentication request packet to an authentication authorization accounting (AAA) server on the network 3. The AAA server responds to the authentication request packet by transmitting an acknowledge packet (PAP_Authentication_ACK) back to the mobile communications terminal 2, which in turn forwards the acknowledge packet to the computer 1. After receiving the acknowledge packet, the computer 1 executes IP Control Protocol (IPCP) negotiation, and thereby begins communication with the network 3.

[0005] The mobile communications terminal 2 performs no processing regarding the authentication request packet other than to forward the request to the AAA server. Also, the mobile communications terminal 2 performs no processing on the acknowledge packet other than to forward the acknowledge packet to the computer 1.

[0006] However, the conventional authentication method for the dial-up networking connection via the terminal has the following problem. After requesting authentication from the AAA server via the terminal 2, the computer 1 must receive an acknowledge packet from the AAA server responsive to an authentication request packet before performing the next step. Thus, the computer 1 does not perform any operation from the time an authentication request is sent until an authentication acknowledgement is received. This time includes the Round Trip Time (RTT) over the unassured mode (UM) interface for the request and acknowledgement. Here, the RTT refers to the time period beginning from when authentication information (e.g., authentication ID, authentication password, etc. for an authentication request of a computer) is transmitted to the network up to the time when a response packet with respect to the authentication request is received. A need therefore exists for a system and a method to reduce the total time required to authenticate a dial-up networking connection via a terminal.

SUMMARY OF THE INVENTION

[0007] Therefore, an object of the present invention is to provide an authentication system and method thereof for a dial-up networking connection via a terminal, whereby, the RRT duration over the UM interface is replaced with the RTT duration over the RM interface, such that the authentication time duration when the computer uses the dial-up network service can be reduced.

[0008] To achieve this and other advantages and in accordance with the purpose of the present invention, as embodied and broadly described herein, an authentication system and method for a dial-up networking connection via a communications terminal is provided comprising: a computer requesting authentication by transmitting an authentication request packet including an authentication ID and authentication password; a terminal monitoring and storing (hereinafter referred to as snooping) the transmitted authentication request packet, forwarding the authentication request packet, and generating an acknowledge packet responsive to the authentication request packet; and a network generating a response packet with respect to the forwarded authentication request packet.

[0009] The foregoing and other objects, features, aspects and advantages of the present invention will become more apparent from the following detailed description of the present invention when taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a unit of this specification, illustrate embodiments of the invention and together with the description serve to explain the principles of the invention.

Figure 1 illustrates an authentication processing procedure for a dial-up networking connection via a terminal in accordance with the conventional art;

Figure 2 illustrates an authentication processing procedure for a dial-up networking connection via a terminal in accordance with the present invention; and

Figure 3 is a flow chart illustrating an authentication method for a dial-up networking connection via the terminal in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0011] Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

[0012] One embodiment of an authentication system and method thereof for a dial-up networking connection via a terminal will now be described in detail with reference to Figures 2 and 3, whereby the RTT duration over the UM interface is replaced with the RTT duration over the RM interface in an authentication processing procedure used by a computer for a dial-up networking connection service, such that the authentication time duration when the computer uses a dial-up networking connection service is reduced.

[0013] Figure 2 illustrates an authentication processing procedure for a dial-up networking connection via a terminal in accordance with the present invention. As shown, an authentication system for a dial-up networking connection via a terminal in accordance with the present invention includes a computer 1 requesting authentication, a terminal 2 snooping an authentication request packet including an authentication ID and password for computer 1, which requests the authentication from the network 3 and generates an acknowledge packet with respect to the authentication request packet, and a network receiving the authentication request packet from the terminal 2 and transmitting an acknowledge packet with respect to the received authentication request packet to the terminal 2.

[0014] Figure 3 describes the operation of the authentication system for the dial-up networking connection via the terminal in accordance with the present invention in detail. The authentication method for the dial-up networking connection via the terminal in accordance with the present invention includes:

inputting an authentication ID and authentication password through a computer (S31);

transmitting by the computer, an authentication request packet having the inputted authentication ID and authentication password to a terminal (S32);

if the authentication ID and password transmitted to the terminal already exist in the previously authenticated IDs and passwords that were previously stored within the terminal (S33),

then generating by the terminal, an acknowledge packet with respect to the authentication request packet and forwarding by the terminal, the authentication request packet to a network (S34),

else storing the authentication ID and password in the terminal (S40);

transmitting by the terminal, the generated acknowledge packet to the computer (S35);

receiving by the terminal, a response packet with respect to the forwarded authentication request packet from the network (S36);

discarding the received response packet when the received response packet is an acknowledge packet (S38); and

notifying the computer and terminating a call request of the computer when the received response packet is a negative acknowledge packet (S39).

[0015] The authentication method for the dial-up networking connection via the terminal in accordance with the present invention will now be described in detail. The description will be made on the assumption that the terminal in accordance with the present invention is a mobile communication terminal (MCT).

[0016] To connect with a network using a dial-up networking connection service, a user inputs an authentication ID and password to a computer 1 and initiates a transmission to a dial-up networking connection service (S31). The computer 1 transmits an AT command to the MCT 2 in order to send a call request. The MCT 2, having received the AT command, transits a Radio Link Protocol (RLP) from an initial NULL state to an Establish state, receives a traffic channel and reports to the computer 1. The computer 1 having received such report initiates a Point to Point Protocol (PPP) setup procedure, and an authentication module of the computer 1 transmits an authentication request packet having the authentication ID and password inputted by the user (S32) to the MCT 2.

[0017] After receiving the authentication request packet, The MCT 2 determines whether the authentication ID and password already exist in authentication information previously authorized and stored in the MCT (S33). The stored authentication information is stored in a nonvolatile memory (e.g., ROM). If the authentication ID and password were previously authenticated and stored, the MCT 2 generates an acknowledge packet responsive to the authentication request packet and forwards the authentication request packet to the network 3 (S34). However, if the authentication ID and password were not previously authenticated, the MCT 2 stores the authentication ID and password by updating the nonvolatile memory with the authentication ID and password. As in the related art, the computer 1 performs the authentication step upon receiving a response packet transmitted from the network (S40).

After generating the acknowledge packet, the MCT 2 transmits the acknowledge packet to the computer 1 (S35). Having received the acknowledge packet, the computer 1 initiates an IPCP negotiation step for the dial-up networking connection without waiting for an acknowledge packet transmitted from the network 3.

[0018] The network 3 generates a response packet responsive to the authentication request packet and transmits the generated response packet to the MCT 2(S36). The MCT 2, having received the response packet, determines whether the response packet is an acknowledge packet (S37). If the received response packet is an acknowledge packet, the MCT 2 simply discards the received response packet because the authentication processing procedure of the computer 1 has already

been completed. However, if the received response packet is a negative acknowledge packet (PAP_Authenticate_NACK), the MCT 2 notifies the computer 1 and terminates the call.

[0019] Therefore, in accordance with the present invention, the RTT duration is reduced because the computer 1 receives an acknowledge packet directly from the MCT 2 on the RM interface rather than indirectly from the network 3 on the UM interface, and the time to complete the authentication process is thereby reduced by 90% or more. The RRT duration over the UM interface is replaced with the RRT duration over the RM interface, such that the authentication time duration when the computer uses the dial-up networking connection service can be reduced.

[0020] As the present invention may be embodied in several forms without departing from the spirit or essential characteristics thereof, it should also be understood that the above-described embodiments are not limited by any of the details of the foregoing description, unless otherwise specified, but rather should be construed broadly within its spirit and scope as defined in the appended claims, and therefore all changes and modifications that fall within the metes and bounds of the claims, or equivalence of such metes and bounds are therefore intended to be embraced by the appended claims.

Claims

1. An authentication system for a dial-up networking connection via a terminal, the system comprising:

   a computer for providing an authentication request, wherein the authentication request comprises an authentication ID and a password, and for communication with a network;
   a terminal for receiving the authentication request, wherein the terminal generates a first acknowledgment responsive to the authentication request, wherein the terminal transmits the first acknowledgment to the computer, and wherein the terminal retransmits the authentication request.

2. The system of claim 1, wherein the terminal further comprises a nonvolatile memory, wherein the nonvolatile memory stores a list of previously authenticated IDs and passwords.

3. The system of claim 1, wherein the terminal compares the received authentication request with the list of previously stored authentication IDs and passwords.

4. The system of claim 3, wherein the terminal generates the first acknowledgment when the authentication ID and password are contained in the list of previously stored authentication IDs and passwords.

5. The system of claim 3, wherein the terminal adds the authentication ID and password to the list of previously stored authentication IDs and passwords when the authentication ID and password are not contained in the list of previously stored authentication IDs and passwords.

6. The system of claim 1, wherein the network receives the retransmitted authentication request.

7. The system of claim 6, wherein the network generates a second acknowledgment to the retransmitted authentication request, and wherein the network transmits the second acknowledgment to the terminal.

8. The system of claim 7, wherein the terminal discards the second acknowledgment when the second acknowledgment is positive.

9. The system of claim 7, wherein the terminal notifies the computer that the authorization is denied when the second acknowledgment is negative.

10. A terminal for authenticating a dial-up connection between a computer and a network wherein the computer provides an authentication request comprising an authentication ID and a password, wherein the terminal compares the authentication ID and a password with a list of previously stored authentication IDs and passwords; and wherein the terminal generates a first acknowledgment responsive to the authentication request when the authentication ID and the password are contained in the list of previously stored authentication IDs and passwords.

11. The terminal of claim 10, wherein the terminal adds the authentication ID and the password to the list of previously stored authentication IDs and passwords when the authentication ID and the password are not contained in the list of previously stored authentication IDs and passwords.

12. The terminal of claim 10, wherein the terminal forwards the authentication request to the network, wherein the network generates a second acknowledgment responsive to the authentication request, and wherein the network transmits the second acknowledgment to the terminal.

13. The terminal of claim 10, wherein the terminal discards the second acknowledgment when the second acknowledgment is positive, and wherein the terminal notifies the computer that the authentication request is denied when the second acknowledgment is negative.

14. An authentication method for a dial-up networking connection via a terminal, the method comprising:

receiving by a terminal, an authentication request including an authentication ID and password from a computer that requests the authentication;
generating by the terminal, a first acknowledgment responsive to the received authentication request; and
transmitting by the terminal, the generated first acknowledgment to the computer.

15. The method of claim 14, wherein the generating step comprises:

determining whether the authentication ID and password of the received authentication request exist in a list of previously authenticated IDs and passwords stored in a nonvolatile memory; and
generating a first acknowledgment with respect to the authentication request when the authentication ID and password of the received authentication request already exist in the list of previously authenticated IDs and passwords.

16. The method of claim 15, wherein, if the authentication ID and password of the received authentication request packet do not exist in the list of previously authenticated IDs and passwords, the authentication ID and password of the received authentication request packet are stored in the nonvolatile memory.

17. The method of claim 14, wherein the generating step further comprises:

forwarding by the terminal, the received authentication request packet to a network.

18. The method of claim 17, further comprising:

generating by the network, a second acknowledgment with respect to the forwarded authentication request.

19. The method of claim 18, further comprising:

receiving by the terminal, the second acknowledgment generated by the network;
discarding by the terminal, the second acknowledgment when the received second acknowledgment is positive, and terminating by the terminal, a call request of the computer when the received response packet is negative; and
notifying the computer that the second acknowledgment is negative.

20. An terminal authentication method for a dial-up networking connection, the method comprising the steps of:

receiving an authentication request including an authentication ID and password from a computer that requests the authentication;
determining whether the authentication ID and password of the received authentication request exist in a list of previously authenticated IDs and passwords stored in a nonvolatile memory;
generating a first acknowledgment with respect to the authentication request when the authentication ID and password of the received authentication request already exist in the list of previously authenticated IDs and passwords; storing the authentication ID and password of the received authentication request packet in the nonvolatile memory when the authentication ID and the password are not contained in the list of previously stored authentication IDs and password;
transmitting the generated first acknowledgment to the computer;
forwarding the authentication request packet to a network;
receiving a second acknowledgment generated by the network;
discarding the second acknowledgment when the received second acknowledgment is positive; and
terminating a call request of the computer when the second acknowledgment is negative notifying the computer that the second acknowledgment is negative.

FIG. 1
CONVENTIONAL ART

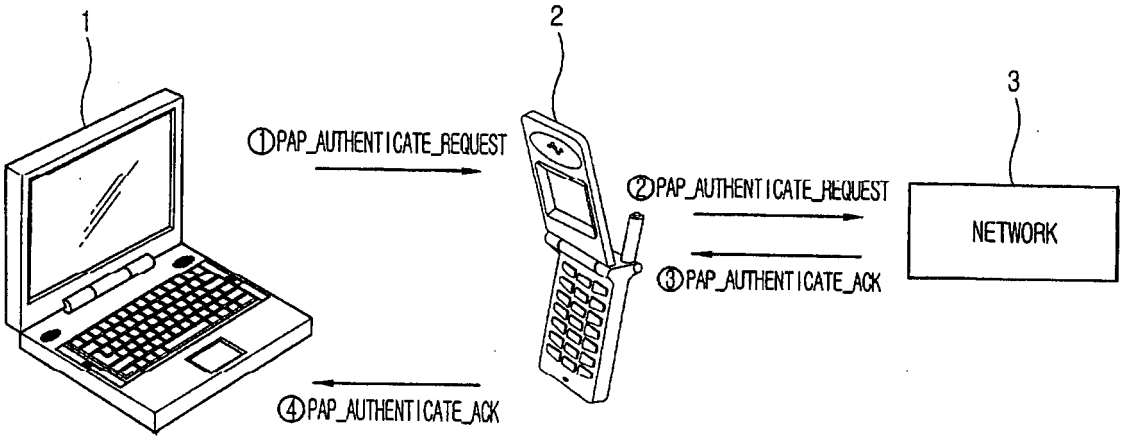


FIG. 2

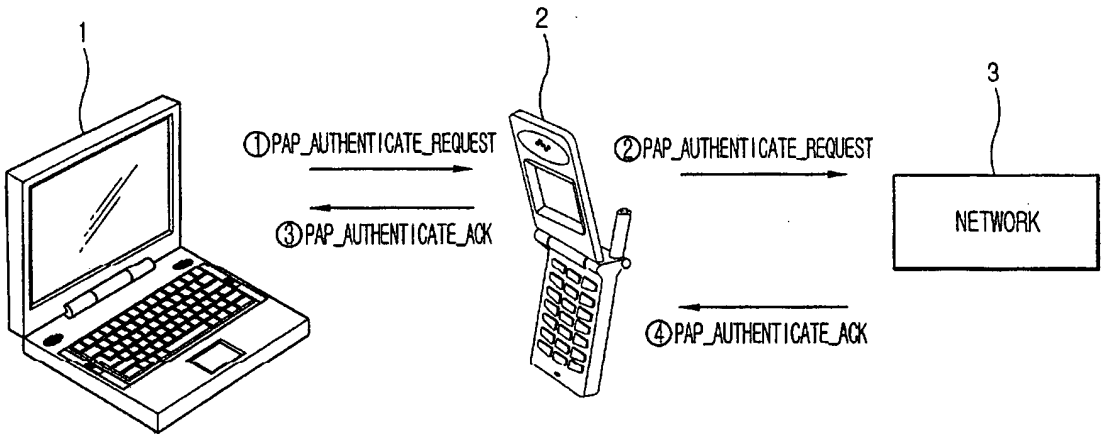
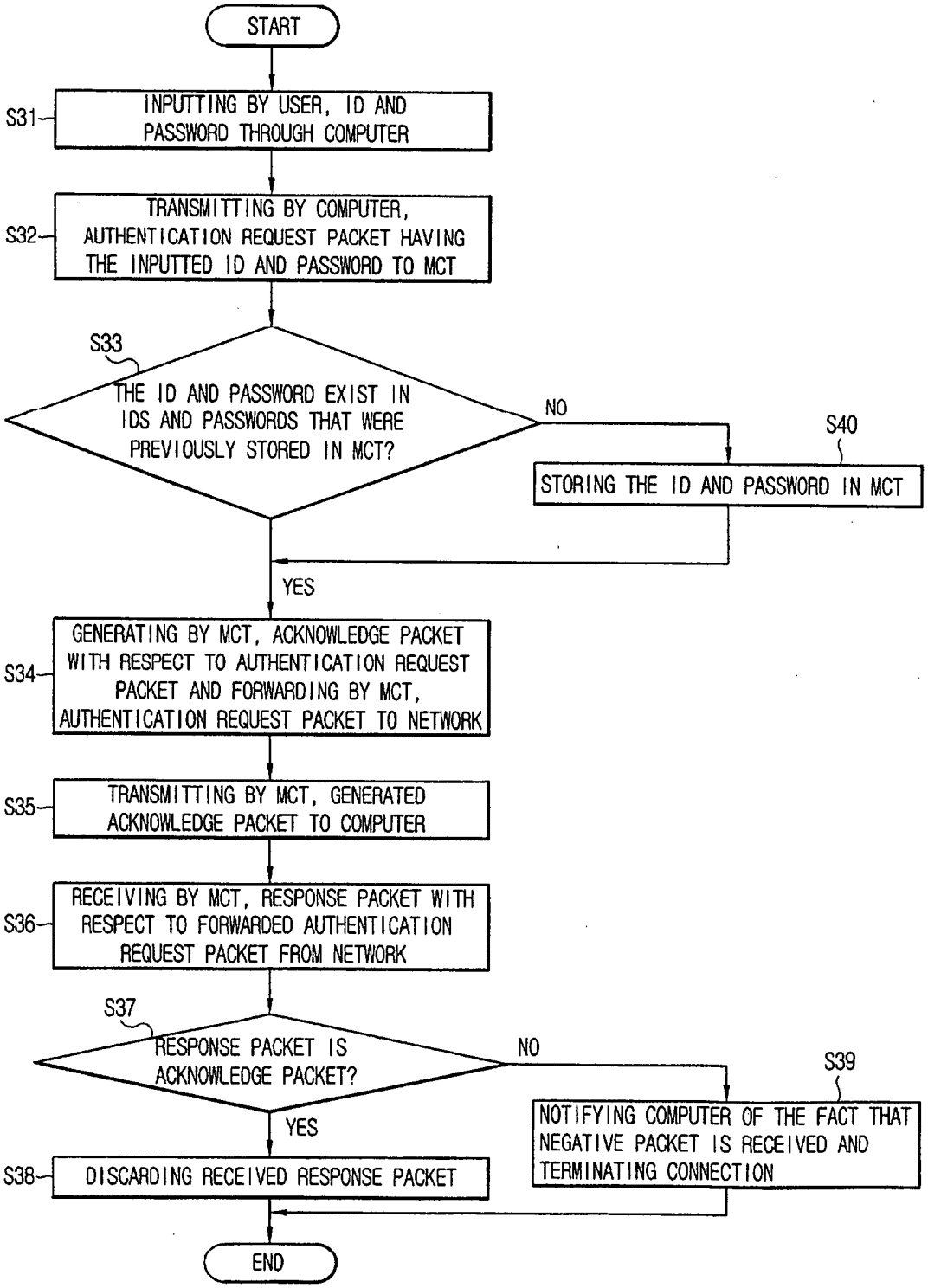

1
2
3
①PAP_AUTHENTICATE_REQUEST
②PAP_AUTHENTICATE_REQUEST
NETWORK
③PAP_AUTHENTICATE_ACK
④PAP_AUTHENTICATE_ACK

FIG. 3


START
S31
INPUTTING BY USER, ID AND PASSWORD THROUGH COMPUTER
S32
TRANSMITTING BY COMPUTER, AUTHENTICATION REQUEST PACKET HAVING THE INPUTTED ID AND PASSWORD TO MCT
S33
THE ID AND PASSWORD EXIST IN IDS AND PASSWORDS THAT WERE PREVIOUSLY STORED IN MCT?
NO
S40
STORING THE ID AND PASSWORD IN MCT
YES
S34
GENERATING BY MCT, ACKNOWLEDGE PACKET WITH RESPECT TO AUTHENTICATION REQUEST PACKET AND FORWARDING BY MCT, AUTHENTICATION REQUEST PACKET TO NETWORK
S35
TRANSMITTING BY MCT, GENERATED ACKNOWLEDGE PACKET TO COMPUTER
S36
RECEIVING BY MCT, RESPONSE PACKET WITH RESPECT TO FORWARDED AUTHENTICATION REQUEST PACKET FROM NETWORK
S37
RESPONSE PACKET IS ACKNOWLEDGE PACKET?
NO
S39
NOTIFYING COMPUTER OF THE FACT THAT NEGATIVE PACKET IS RECEIVED AND TERMINATING CONNECTION
YES
S38
DISCARDING RECEIVED RESPONSE PACKET
END